DOCUMENT IMAGING WORKPROGRAM

CHAPTER 17WP

(FILE NAME ON DISK # 3= IS–WP#12)

COMMENTS

This section is intended to determine the adequacy of the institution control over its electronic document imaging systems operations. The levels of controls will depend on the degree of reliance the institution places on its imaging operation. Systems could vary from small isolated local scanning/recordkeeping to financial, customer database information files, and highspeed check processing. The imaging system operations should be reviewed in consideration of the importance of the information/data to the institution rather than its size. The examiner should document any findings, especially those which do not satisfy the recommendations in the *1996 FFIEC IS Examination Handbook*.

Tier I

MANAGEMENT CONTROLS

1. Evaluate the adequacy of general controls that have a direct effect on the imaging system, such as cost benefit studies, physical security, data security, documentation, error handling, program change procedures, system recoverability, and vital records retention.

2. Evaluate the overall adequacy of controls for the integrity documents scanned through the system (accuracy and completeness). These documents are converted from paper to a machine readable format and must remain in the system during conversion.

3. Ensure that appropriate controls are in place prior to destruction of source documents (e.g., shredded) after being scanned through the imaging system.

4. Ensure that compliance with regulations and standards is being enforced by management.

5. Ensure that the imaged departments or applications have been incorporated into the financial institution's contingency planning procedures.

6. Determine if a segregation of duties is in place, where the imaging occurs. This ensures that the work of one person is reviewed by another, that a specialization of tasks has been created, and that any instances of fraud are inhibited.

TRAINING

7. Determine whether an adequate technical training program exist for users, operators, and staff.

CONCLUSIONS

8. Review the results of work performing in this section and in sections for Examination Planning, Internal/External Audit, and Management (Chapters 3, 8, and 9). If the results reflect significant control deficiencies, or you are unable to reach a conclusion, perform additional procedures, as necessary, in other relevant sections. Workpapers should reflect the examiner's reasons for the performance or exclusion of Tier II procedures.

9. Discuss with management:

   a. Violations of law, rulings, regulations, or significant internal control deficiencies.

   b. Recommended corrective action for deficiencies cited.

   c. Management's proposed actions for correcting deficiencies.

10. Assign rating (see Chapter 5 for additional information.)

11. Prepare an index of workpapers for this section of the workprogram.

12. Prepare a separate summary findings worksheet for this section of the workprogram. The summary should include a discussion of IS control strengths, weaknesses, deficiencies, or other problem and/or high risk areas. Also include important facts, findings, examiner conclusions, and, if applicable, recommendations. Present conclusions about the overall condition of IS activities in this workprogram area. In addition, provide any additional information that will facilitate or enhance future examinations.

13. Prepare draft report comments for reportable findings and/or matters to be included in the administrative section of the ROE.

Examiner | Date

____________|________

Reviewer's Initials

Tier II

Negative responses/determinations should be discussed with management. Their remedy, compensating controls, and your comments must be recorded.

MANAGEMENT CONTROLS

1. Has an imaging system been installed at the institution? Describe its functions and the responsibilities of the department/staff.

2. If no, explain whether issue is being explored and studied, relative to future bank technologies.

3. If yes, explain whether it complements the financial institution's current technology structure.

4. If yes, explain how the system is/was justified.

5. If installed, obtain dates.

6. Determine whether the stated benefits are obtained.

7. For the imaging project, assess whether management developed a set of clear, manageable and measurable goals, relative to the processing environment, technology choices, and external/internal influences.

8. Review the overall business components of the process:

   a. Strategy.

   b. Application Selection.

   c. Implementation.

   d. Roll-out.

9. Determine whether all pertinent personnel have been involved.

10. Identify the risks that were taken.

11. Determine whether the workflow is installed and operating correctly.

12. Prior to the introduction of imaging, determine whether a pilot team assessed controls, system benefits, etc.

13. Determine which of the following comprises this pilot team:

    a. End Users.

    b. MIS.

    c. Audit.

    d. Data Security.

    e. Bank Operations.

14. Verify whether management contacted any organization to obtain assistance on imaging guidelines. (Note: Examples of such organizations are Association for Information and Image Management; Department of Defense; American Banking Association; the American National Standards Institute; National Automated Clearing House Association; National Association for Check Safekeeping; and the Electronic Check Clearing House).

INFORMATION SERVICES

15. Describe how the Imaging System communicates with the host and whether the host is:

    a. LAN.

    b. T-1.

16. Determine the imaging system's capacity and future growth capability.

17. Describe the topology being used and whether it is:

    a. Mini-based.

    b. PC-based.

    c. Mainframe-based.

18. Identify the vendor and who assessed its reliability. (Note: If Information Services personnel have retained files on the vendor analysis, review this file to determine the justification of selecting a particular vendor).

19. Since companies use different imaging standards, define the imaging standard being used.

20. Describe the migration issues that have been addressed relative to moving to the next generation.

21. Describe how document conversion is being accomplished. Examples include: back-file conversion; as you touch; and only new documents.

22. Determine whether plans exist to share documents between departments and whether branches are using imaging (teller and customer service areas accessing images through desktop computers).

23. Describe the back-up procedures, including:

    a. Dual optical disks.
    b Tape back-up.
    c. Optical disks.
    d. Digital audio tape (DAT).

24. Describe the financial institution's disaster recovery procedures for imaging, including:

    a. Recovery at the institution’s own site.
    b. Recovery at the vendor’s site.
    c. Another company, completely separate from the bank.

25. Identify which of the following performs the hardware maintenance:

    a. End-user.
    b. Information services.
    c. Vendor.
    d. Other.

26. Identify which of the following performs the programming and on-going programming enhancements:

    a. End-user.
    b. Information services.

c. Vendor.

d. Other.

27. Identify which of the following provided and continues to provide programming documentation:

a. End-user.

b. Information services.

c. Vendor.

d. Other.

29. Describe whether users understand the technology and have received training on imaging.

30. Determine whether both users and Information Services personnel are satisfied with the quality control of scanned documents.

31. Evaluate whether the financial institution acquired any PC-based systems that analyze the condition of checks (if check processing imaging occurs), prior to the information being imaged.

32. Describe the recovery of bad images by using:

a. Re-scan ALL.

b. RE-scan ONLY defective images.

33. Describe the recovery from hard/optical disk by using:

a. Back-up tape.

b. Optical copy.

c. Re-scan all documents.

34. Describe how the indexing of documents is performed. (Note: Proper indexing at the time of capture is critical for retrial and authorizing access levels to documents. The integrity of indexes must be carefully maintained to ensure that electronic documents can be located and accessed quickly and accurately. Poorly designed indexes can result in lost documents).

a. After each document is scanned.

b. After all documents are scanned.
c. Indexing controls.

35. Determine whether the imaging hardware is interchangeable with other vendors hardware (i.e., imaging hardware is used to display or print the storage).

36. Determine whether the imaging software is interchangeable with other vendors software (i.e., imaging software is used to locate the stored image).

37. Determine whether the financial institution can migrate to the next generation of hardware.

38. Determine whether the financial institution can interchange documents with other vendor systems through such devices as:

    a. Fax.
    b. LANs.
    c. Wide area networks.

39. Describe whether plans exist to share documents between departments.

40. Assess whether management from information technology or top management conferred with the bank's legal department to determine if documents should be destroyed after the Imaging process was completed.

41. Define the retention period for source documents. (Note: The law may vary from state to state).

42. Define the retention period for image documents. (Note: The law may vary from state to state).

43. Evaluate whether the financial institution can prove in court that documents cannot be changed prior to storing on optical disk.

44. Define the audit trail detention period.

45. Determine if vendors who provide imaging service were asked to sign non-disclosure agreements.

SECURITY CONTROLS

46. Obtain an understanding of access security controls. Examples include:

    a. Maintaining a Data Security Administration function.

    b. Maintaining written procedures for information security relative to imaging.

    c. Controls over an electronic imaging file, preventing the manipulation of bytes.

    d. Controls over the image underlying index, preventing the writing over an existing image.

    e. Controls over the index file, preventing this file from being tampered with or damaged. Such damage or destruction would severely hinder the system's ability to locate and retrieve data.

47. Determine if security violation and other pertinent reports are being reviewed and ensure that other controls are in place for: (Note: Mainframe software security, such as RACF or ACF2, can add a level of security on the index data in imaging. Incorporating imaging with adequate access controls requires implementing independent layers of software security).

    a. Password length.

    b. Maximum number of logon attempts, before user ID is suspended.

    c. Mandatory changes of user passwords (e.g., every 30 days).

    d. DES encryption on disk and storage.

    e. Limiting users to authorized applications.

    f. Limiting users to authorized data/records.

    g. Alterations of data by authorized users.

    h. Terminal time out feature for inactivity.

OTHER CONTROLS

48. Determine if controls are in place to prevent the system from booting from other media (e.g., floppy disk) or access any other disks, bypassing security controls.

49. Ascertain if controls exist over such sensitive software as:

    a. Software that can modify images.

    b. Software that can cut and paste.

    c. Software that can alter or bypass security.

50. Determine whether image back-ups are stored away from the primary location of the financial institution and whether they may be performed by making dual optical disk copies.

TRAINING

51. Determine weather policies and procedures are in place to ensure adequate technical training of the users, operators, and staff.

52. Determine whether adequate documentation exists for use in training and as a reference material for all systems and application functions.

53. Assess whether security and control concerns are part of the education and training programs for the users, staff, and operators.

54. Evaluate how corporate policies are communicated to personnel relative to training programs.

55. Assess how changes to the system are accounted for in training and education programs, including documentation and work aids.

56. Proceed to procedure 8, Tier I.

Examiner | Date
___________|________

Reviewer's Initials